#30

ADVANCING HUMAN CAPABILITIES acm THROUGH INFORMATION TECHNOLOGY

February 12, 1997

Office of U.S. Public Policy

Nancy Crowe
Regulatory Policy Division
Bureau of Export Administration
Department of Commerce
Room 2705
14th Street and Pennsylvania Ave., N.W.
Washington, D.C. 20230.

Docket No. 960918265-6366-03

Dear Ms. Crowe

The United States Public Policy Committee for the Association for Computing (USACM) welcomes this opportunity to submit our views on the Interim Rule issued by the Department of Commerce with regard to "Encryption Items Transferred From the United States Munitions List to the Commerce Control List." The USACM believes it is in the best interest of the U.S. government to promote the widespread use of strong encryption. From our perspective the Interim Rule fails to recognize the legitimate needs and interests of academic, professional, scientific, and ordinary users of telecommunications technology. Thus, the Interim Rule must be modified before it can resolve the many problems with the current export controls on encryption technologies.

Introduction and Summary

The Association for Computing is an international professional society whose 76,000 members (60,000 in the U.S.) represent a critical mass of computer scientists in education, industry, and government. The USACM provides a means for promoting dialogue on technology policy issues with United States policy makers and the general public. We have identified a number of serious problems with specific provisions of the Interim Rule.

As a professional society of computer scientists which produces a number of peer-reviewed technical journals, we are concerned that the Interim Rule will hamper both communication and education in our field. Part 7.34.3 (b)(3) which refers to the distinction between printed and electronic publications of cryptographic materials is unworkable under the new paradigms of electronic publishing and communications. Electronic media, including the World Wide Web, listserves, Usenet news groups, and video conferencing are becoming the prominent means by which scientists communicate. Provisions of the Rule, specifically Parts 7.34.9 and 744.9, which affect teaching cryptography to foreign students are vague and contradictory. Educational environments are not limited to academic institutions but also occur in national and industry labs and by distance education. Restrictions on cryptography exports must not interfere with the traditional freedom of access over digital networks which is indispensable to maintain motivated and effective academic and research communities.

We also believe that the development of public policies and technical standards for communications technologies, such as a Key Recovery Infrastructure (KRI), raise vital issues of privacy, competitiveness, and scientific innovation. Parts 740.8 and 742.15 raise a number of troubling issues for the computing community. We believe it is unwise for the Commerce Department to link relaxing export controls on 56-bit encryption to the development of a KRI as both the desirability and the feasibility of such a system remains uncertain. Key recovery products have not yet been subject to the vigorous testing necessary for a proposed standard and there is little understanding of how such a system would operate and what controls would be needed to ensure that it remained secure. Also, Supplement No. 7 to part 742 (which requires that businesses who wish to export 56-bit encryption before 1998 submit a biannual business plan for developing key recovery products) will stifle the innovation of new cryptography technologies and discourage the process of scientific innovation. We believe the Commerce Department should not promulgate regulations which prohibit U.S. research and development from responding to market demands and limit the ability of Americans using new on-line services to protect their privacy.

Analysis

The USACM has identified electronic publication, education, research and development, key recovery, and privacy as problematic areas which need addressing. We have outlined our concerns below:

Electronic Publishing

It is unreasonable and unconstitutional to distinguish between printed and electronic distribution of encryption source code as set forth in the note to Part 7.34.3 (b)(2) and (b)(3). A Federal Court in California has ruled in Bernstein v. U.S. Department of State that source code is speech and is thus protected under the first amendment. This distinction is also currently being challenged in a federal court in the District of Columbia in Karn v. U.S. Department of State. The USACM joined the Electronic Privacy Information Center, the American Civil Liberties Union, and the Internet Society in submitting an Amici Curiae brief in the case which argued that such language is an impermissible regulation aimed at the suppression of expression. As computer scientists we see no practical reason why the Commerce Department should insist on creating a distinction when one does not exist.

The ACM is the publisher of numerous scientific publications and conference proceedings. They range from our flagship journal **Communications of the ACM** (CACM) to the on-line, peer-reviewed journal **Experimental Algorithms**. All 76,000 members of ACM, including 15,000 members overseas, receive CACM by mail and have access to ACM's on-line publications. ACM foresees a time when all its publishing will be electronic and on-line. At that time, it will need interoperable encryption technology available in the U.S. and in its mirror sites abroad to dispense its material. Its subscribers worldwide will need access to secure, commercial encryption as well.

An article which described the development of a new cryptographic algorithm would likely appear in one of the many technical journals or conference proceedings published by ACM or the Institute for Electronics and Electrical Engineers (IEEE), another international professional society. In fact a number of the groundbreaking articles in the field of cryptography science were originally published by ACM and IEEE. Publication of encryption algorithms is extremely important to the field of cryptography. In order for an algorithm to be trusted, it must be challenged. To do that, the code must be made widely available. Foreign members of ACM will be unable to access in electronic format the same articles they currently receive in the printed journal. And, it is technically impossible, at this late date, to partition ACM's publications into distinct paper and electronic (hence encryptable) media.

Electronic communications, including the World Wide Web, list serves, Usenet news groups, and video conferencing are becoming the prominent means by which scientists communicate. Science is a global pursuit and there exists a open communications network between scientists in different countries. Part 734.2 which prohibits making cryptographic software available outside the U.S. will not only eliminate this international communication but also technical communication among U.S. scientists. In electronic communications it is not always clear to whom the information is being transmitted. WWW sites and Usenet news groups are accessible by anyone with a modem. Video conferences can be retransmitted overseas and moderated listserves are difficult to control. The Interim Rule refers to an individual taking "precautions adequate to prevent unauthorized transfer of such code outside the U.S." It is our belief that it would be impossible to be certain of any precautions taken. This will effectively eliminate all communications on electronic media that describe or discuss cryptographic source code.

We believe the interim rule must be revised to eliminate the distinction between printed and electronic source code and to allow for open communications within scientific communities. Restricting these communications will retard the evolution of the science and the development of new algorithms and cryptographic devices.

Education

Many ACM members are computer science professors and teachers, so we are concerned about the contradictions in the proposed regulations with regards to education. A number of fields and sub-fields address cryptography as part of their curricula. Part 734.9 states that "Educational Information" is not subject to the new regulations if it is "released by instruction in catalog courses and associated teaching laboratories of academic institutions." Computer science, mathematics, engineering, and electronic security may all include technical instruction in encryption technologies and would be covered in U.S. university classrooms. However, questions arise with regard to distance and home or overseas education because of Part 744.9. It states that "No U.S. person may, without a license from BXA, provide technical assistance (including training) to foreign persons with the intent to aid a foreign person in the development or manufacture outside the United States..." While Part 744.9 defines a U.S. person it does not define "technical assistance" or "training." It is uncertain whether a U.S. professor teaching a course in which foreign students are registered, or teaching a course in cryptography overseas would be "training" a foreigner to develop a cryptographic device if the course work was more detailed than "a discussion of information about cryptography." This would affect course studies as disparate as 'number theory' and 'local area networks'.

Also, educational environments are not limited to academic institutions but are also found in national and industry labs. Many computer scientists receive their first hands on training after they graduate from their University. It is unclear whether this "training" or "technical assistance" is in violation of the Interim Rule. The intent of the training is give the new employee the practical tools necessary to participate in the field of cryptography science, and is not necessarily intended to be project or employer specific. While the General prohibition in Part 744.9 discusses the meaning of intent as applied to an academic setting, it is not clear if "academic setting" can be applied to instruction which occurs outside of the University environment.

The argument made previously with regard to digital media also applies to education. As part of their course work, students often use electronic media as resources (WWW, digital libraries, CD-ROMs), as a communication device for the class outside the classroom (electronic mail, listserves), and to learn from listening to the discussions among research scientists (Usenet groups, listserves). Part 7.34.3 (b)(3) which covers encryption source code in electronic form or media will restrict these types of educational instruction. Instructors will be unable to take advantage of digital media in their courses. Students studying cryptography will be unfairly disadvantaged as they will be unable to access valuable resources even in the process of furthering their education.

The USACM believes the contradictions in Parts 7.34 and 744.9 must be resolved in a clear manner so educators are not required to reduce the quality of their courses for fear of misinterpreting the Interim Rule. Specifically, "academic setting," "training," and "technical assistance" must be defined, and distance education, and academic research and communication must be addressed.

Research and Development

Encryption policies must reflect the needs of the global market. The international demand for products which incorporate strong cryptographic tools is growing. Such products are widely available and produced by a number of nations. U.S. scientists have been prominent in the development of current encryption technologies. The field has developed though research and development efforts along many different tangents, only one of which describes key recovery products. There is little evidence that the demand for cryptography tools is limited to those products which incorporate key recovery protocols. Part 742.15 (which states that businesses must submit a business plan for the development of key recovery products before they may export 56-bit software; the license must be renewed biannually until 1998 when only key recovery products will be allowed for export) will restrict the U.S. to producing only products which incorporate KRI protocols.

Mandating that businesses develop key recovery products will also impede the natural market development of novel and innovative systems. Part 740 hypothesizes that a worldwide KRI will be desirable, feasible, and in place by 1998. However it is unclear whether key recovery is the best alternative. Research along new tangents will continue in non- industry and non-U.S. settings. A new protocol may be discovered which is considered a better choice for a worldwide infrastructure. There will exist a great market demand for variety in choosing a security system to fit the needs of the distinct commercial group. If this happens U.S. scientists and industry will be at a disadvantage as they will have only a core competence in key recovery protocols as per Part 740.8.

There are a variety of commercial groups interested in utilizing the Internet for business interactions and transactions. Without interoperable encryption programs, commercial needs in an increasing global environment cannot be met. Supplement No. 4 to Part 742 states that a product can not interact with another product whose key recovery system has been "altered, bypassed, disabled, or otherwise rendered inoperative." This will be a major source of problems for researchers and educators, as well as government and commercial institutions. The result of a system not being able to talk to another system because of an intentional or accidental disabling of the KRI protocols can have a very large impact on telemedicine, research, government operations, and commercial enterprises.

The USACM believes the Interim Rule should be rewritten to avoid dissuading innovation and development and eliminating the U.S.'s core competency in cryptography. It should also recognize the need for consistency in interoperable systems.

Key Recovery

The USACM recognizes that there is a real market demand for key recovery products from business and government employers. However, the viability of a KRI has not yet been determined. It has not yet been subject to the vigorous testing necessary for a proposed standard. There is little understanding of how such a system would operate and what controls would be needed to ensure that it remained secure. Part 740 describes the development of a Key Recovery Infrastructure within two years. We believe it is unwise for the United States to insist on the development of a untested, unproved technology for a worldwide infrastructure. The National Research Council report stated that a feasibility study needed to be performed on a smaller scale before key escrow could be seriously proposed for commercial applications. We believe this warning applies to KRI as well. While key recovery tools may be appropriate in some settings, we believe it would be wrong to impose such restrictions on users or businesses and the Interim Rule should not dictate that businesses limit their research to a potentially unworkable system.

Privacy

The USACM believes that certain principles should be reflected in a national cryptography policy. Encryption should be used for privacy protection and to encourage the development of technologies and institutional practices which will provide real privacy for the future users of the NII and real security for the protection of the system. The USACM believes that transferring the regulation of cryptography to the Commerce Department could establish United States leadership in protecting the privacy rights of its citizens. However the Interim Rule fails to do that.

Conclusion

We recognize that the government has a legitimate interest in protecting national security. However, whether or not the worldwide infrastructure is achieved, the role of national security agencies will remain difficult. The government's proposal to balance national security, business, and privacy interests by creating a Key Recovery Infrastructure within the next two years is overly aggressive. We suggest that the development of a policy that serves the long term interests of our nation's security will not be one based on a Key Recovery Infrastructure, but rather one that anticipates the widespread availability of strong encryption and the multifaceted demands of a global economy. Toward that end, the interests in protecting open research within the U.S. academic community will be crucial.

Sincerely,

Barbara Simons

Barbara Simons, Ph.D
Chair, United States Public Policy Office for the
Association for Computing

The ACM, founded in 1947, is an international non-profit educational and scientific society dedicated to the development and use of information technology, and to addressing the impact information technology has on the world's major social challenges. The Association's activities include the publication of scholarly journals and the sponsorship of special interest groups (SIGS) in numerous disciplines. ACM has 76,000 members. The 60,000 who reside in the United States are academic, professional, scientific, and ordinary users of telecommunications technology and have a strong interest in the development of sound encryption policies. The USACM provides a means for promoting dialogue on technology policy issues with United States policy makers and the general public. We respond to requests for information and technical expertise from United States government agencies and departments, seeks to influence relevant United States government policies on behalf of the computing community and the public, and provides information to the ACM on relevant United States government activities.